Transmission Media (Communication media)

These are the means by which a communication signal is carried from one system to another. These media can carry information from a source to a destination. The transmission media can usually be free space such as: satellite, microwave, radio and infrared systems, metallic cables such as: twisted pair, or coaxial cable, or fiber-optic cable.

In telecommunication, transmission media can be divided into two broad categories:

i. Guided transmission media

ii. Unguided transmission media

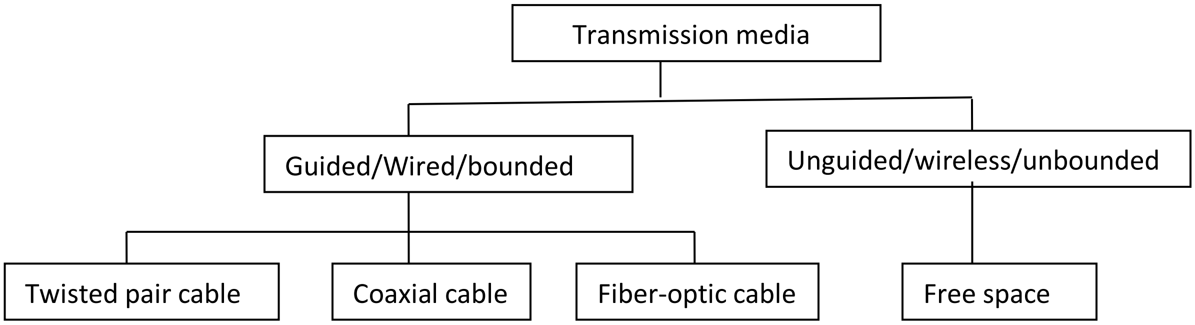
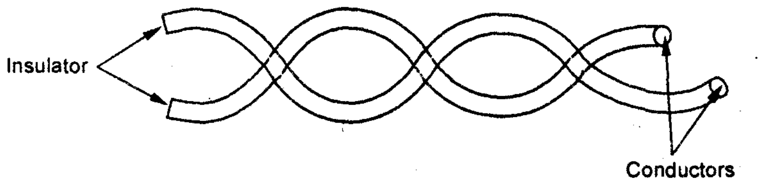


Fig: Classes of transmission media

Guided Transmission Media

Guided Transmission media uses a cabling system that guides the data signals along a specific path. They provide the physical path way for the transmission of the data from the source to the destination. The data signals travelling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductor that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transport signals in the form of light. Guided Media are also known as Bound media or wired media.

Twisted pair



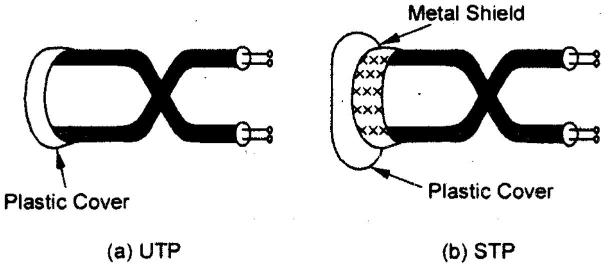
A twisted pair consists of two insulated strands of conductors (normally copper), each with its own plastic insulation, twisted around each other to form a pair. One of the wires is used to carry signals to the receiver and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wire, interference (noise) and crosstalk may affect both wires and create unwanted signals. Thus they are twisted to maintain the balance.

The degree of reduction in noise interference is determined specially by the number of turns per foot increasing the number of turns per foot reduces the noise interference.

The most common twisted pair cables used in communications is:

a) Unshielded twisted pair (UTP)

b) Shielded twisted pair (STP)



a) Unshielded twisted pair (UTP):

As the name implies UTP cables contain no shielding mechanism. It is the most common twisted pair cable used in communication and LAN. These cables are used on Ethernet 10 Base T and can also be used with token ring. It uses the RJ line of connectors (RJ 45, RJ 11 etc).

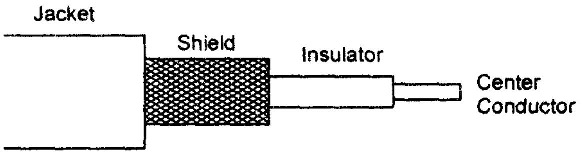
These cables are less expensive and light in weight in comparison to STP. They are more common and can easily be found in the market. However, they are more prone to noise and electromagnetic interference.

b) Shielded twisted pair (STP)

STP cable has a metal foil or wire braid-mesh covering that encases each pair of insulated conductors. To further improve noise rejection, a foil or wire braid shield is wound around the twisted pair. This shield can be moves around individual pairs or around a multi pair conductor.

Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. Thus they are less common and are difficult to find in the market in comparison to UTP.

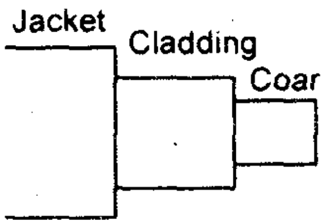
Coaxial cable:



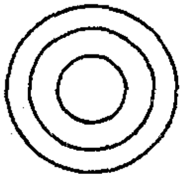
Coaxial cable made up of two conductors that share the same axis. The sender is a copper wire that is insulated by plastic cover called the jacket and then wrapped with an outer conductor usually wire braid. This outer conductor around the insulation serves as an electrical shielding for the signal being carried out by the inner conductor. A tough insulating plastic tube outside the outer conductor provides physical and electrical protection. The inner conductor is held inside the insulator with the other conductor waves around it providing a shield. An insulating protective coating called a jacket covers the outer conductor.

The outer shield protects the inner conductor from outside electrical signals. The distance between the outer conductor (Shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance. Typical impedance for coaxial cables is 75 ohm for cable TV, 50 ohm for Ethernet thin net and thick net. The excellent control of the impedance characteristics of the cable allow higher data rates to be transferred than twisted pair cable.

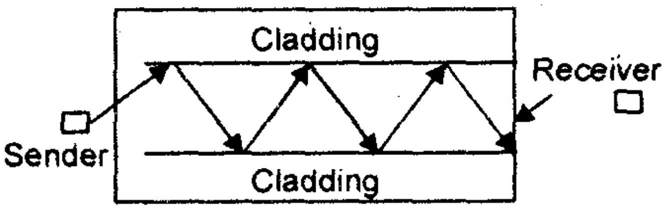
Optical Fiber:



Side View



End View



Optical Fiber

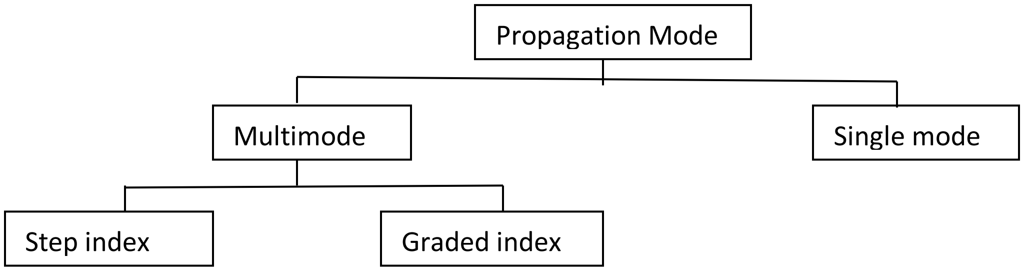
A fiber optic cable is made up of light conducting glass or plastic fibers. It can carry data signals in the form of pulses of light. The plastic core cables are easy to install but do not carry signals as far as glass cables.

Optical fiber consists of thin glass fiber that can carry information at frequencies in the visible light spectrum. The typical optical fiber consists of a very narrow strand of glass called the cladding. A typical core diameter is 62.5 microns. Typically cladding has a diameter of 125 minors. Coating the cladding is a protective coating consisting of plastic, it is called the jacket.

Optical fibers use the concept of total internal reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two material must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Propagation Mode:

Current technology supports two modes for propagation of light along optical channels; each requiring fiber with different physical characteristics. It can be shown as:



Multimode:

It is so named because multiple beams from a light source moved through the core in different paths. How these beams move within the cable depends on the structure of the core as in figure below:

a) **Multimode Step-index:**

In this mode, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core ad cladding. At the interface there is an abrupt change due to a lower density, this alters the angle of the beam’s motion. The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passed through the fibers.

b) **Multimode Graded-index:**

It decreased this distortion of the signal through the cable. The word index here refers to the index of the refraction. We know that the index of refraction is related to the density. A graded-index fiber, therefore, is one with varying density. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

c) Single mode:

Single mode use step-index fiber and highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fibers itself is manufactured with a much smaller diameter than that of multimode fiber and with substantially lower density. The decrease in density results in a critical angle i.e. close enough to 90^0 to make the propagation of beam almost horizontal. In this case, propagation of different beams is almost identical and delays are negligible. All the beams arrive at the destination together and can be recombined with little distortion to the signal.

Advantages of optical fibers

(i) Small size and light weight: The size of the optical fibers is very small. Therefore a large number of optical fibers can fit into a cable of small diameter.

(ii) Easy availability and low cost: material used for the manufacturing of optical fibers is “Silica glass”. This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.

(iii) No electrical or electromagnetic interference: Since the transmission takes place in the form of light ray, the signal is not affected due to any electrical or electromagnetic Interference.

(iv)Large Bandwidth: As the light rays have a very high frequency in GHz range, the bandwidth of the optical fiber is extremely large.

(v) Resistance to corrosive material: Glass is more resistance to corrosive material than copper.

(vi)Other advantages: No cross talk inside the optical fiber cable. Signal can be sent up to 100 times faster.

Disadvantages:

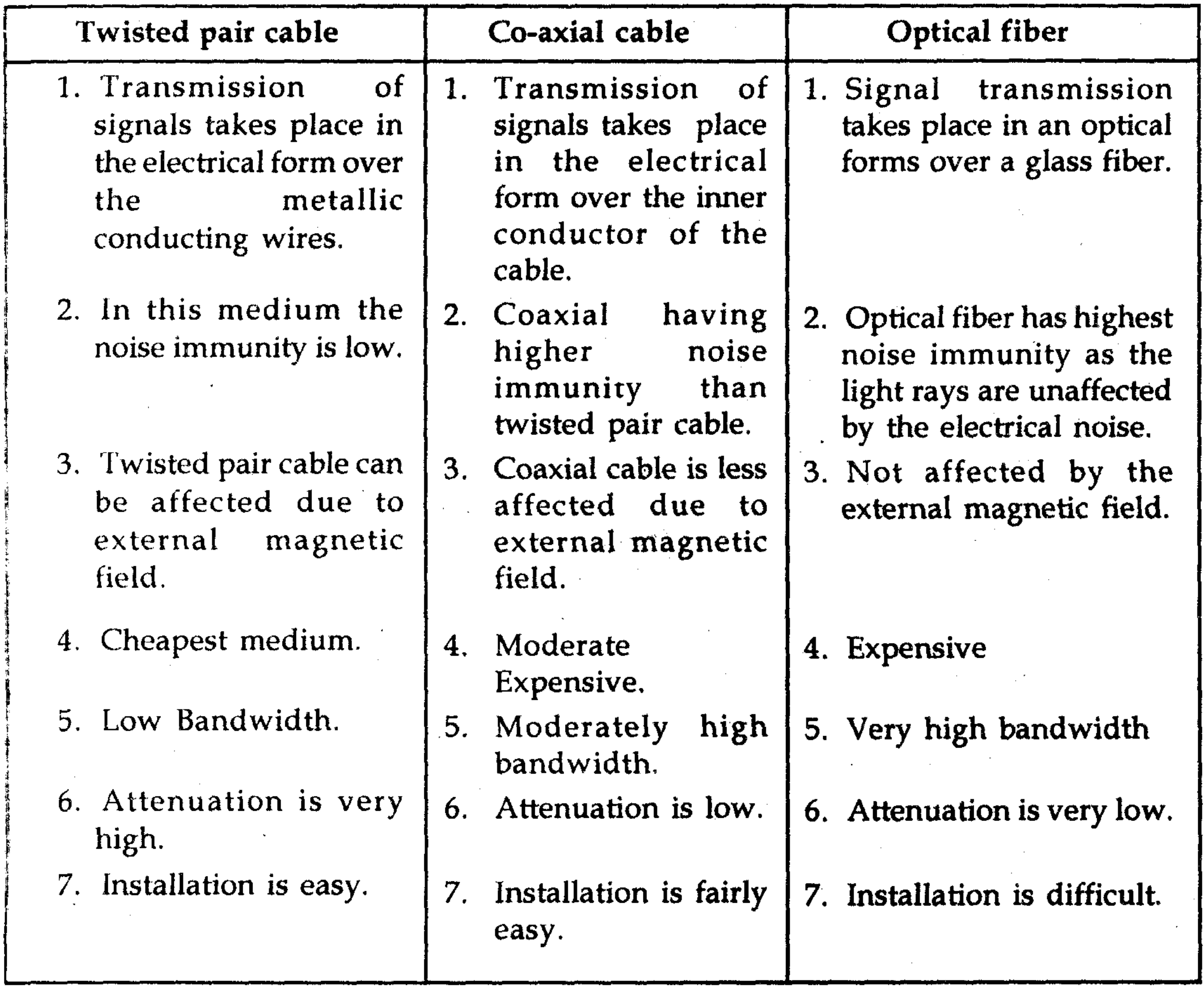
(i) Installation and maintenance: Since it is relatively new technology, its installation and maintenance requires expertise that is not yet available everywhere.

(ii) Unidirectional light propagation: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

(iii) Cost: The cable and the interface are relatively more expensive that those of other guided media i.e. one time cost is high.

(iv) Requires special technical man power to install and maintain.

Comparison: twisted pair, co-axial cable and fiber optics



Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires.	1. Transmission of signals takes place in the electrical form over the inner conductor of the cable.	1. Signal transmission takes place in an optical forms over a glass fiber.
2. In this medium the noise immunity is low.	2. Coaxial having higher noise immunity than twisted pair cable.	2. Optical fiber has highest noise immunity as the light rays are unaffected by the electrical noise.
3. Twisted pair cable can be affected due to external magnetic field.	3. Coaxial cable is less affected due to external magnetic field.	3. Not affected by the external magnetic field.
4. Cheapest medium.	4. Moderate Expensive.	4. Expensive
5. Low Bandwidth.	5. Moderately high bandwidth.	5. Very high bandwidth
6. Attenuation is very high.	6. Attenuation is low.	6. Attenuation is very low.
7. Installation is easy.	7. Installation is fairly easy.	7. Installation is difficult.

II) Unguided Media

The unguided media is the wireless media. It simply transports electromagnetic waves without using any physical conductor. Signals are normally broadcast through the air and thus are available to anyone who has the device capable of receiving them.

Wireless transmission

Wireless communication is the transfer of information over a distance without the use of electrical conductors or “wires”. The distances involved may be short (a few meters as in television remote control) or very long (thousands or even millions of kilometers for radio communication). Wireless communication is generally considered to be a branch of telecommunications.

Three ways for wireless data propagation

(i) Radio wave

(ii) Microwave

(iii) Infrared

Ground propagation

Radio waves travel through the lowest portion of the atmosphere, hugging he earth. These low frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal, that is the greater the power, the greater the distance.

Sky propagation

Higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to earth. This type of transmission allows for greater distances with lower power output.

Line-of-sight propagation

In line-of-sight (LOS) propagation very high frequency signals are transmitted in straight lines directly from antenna-to-antenna. Antenna must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth. LOS propagation is trekking because radio transmission cannot be completely focused.

Radio waves:

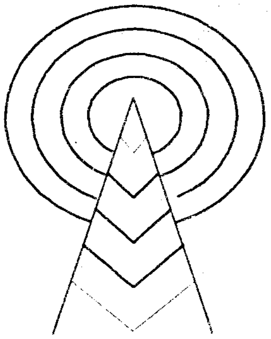
Electromagnetic wave ranging in frequencies between 3 KHz and 1GHz are normally called radio waves.

Radio waves are omnidirectional when an antenna transmits radio waves they are propagated in all directions. This means that sending and receiving antenna do not have to be aligned. A sending antenna can send waves that can be received by any receiving antenna. This omnidirectional property is the disadvantage that the radio waves transmitted by tone antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Radio waves particularly those waves that propagate in sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

Radio waves particularly those of low and medium frequencies can penetrate walls. It is an advantage because; an AM radio can receive signals inside a building. It is the disadvantage because we cannot isolate a communication to first inside or outside a building. The radio waves band is relatively narrow just under I GHz, compared to the microwave band. When this band is divided into sub-band, the sidebands are also narrow, leading to a low data rate for digital communications.

Almost all the entire band is regulated by authorities using from the authorities. Radio waves use omnidirectional antennas that send ourt signals in all directions based on the wave lengths, strength and purpose of transmission, we can have several types of antennas.



Omnidirectional Antenna

Applications:

The directional characteristics of radio waves make them useful for multicasting. In which there is one sender but many receiver. Radio waves are used multicast communications such as radio (AM, FM), TV, paging system, and cordless phones.

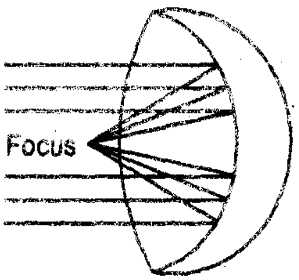
Microwaves:

Electromagnetic waves having frequencies between 1 GHz and 300 GHz are called microwaves.

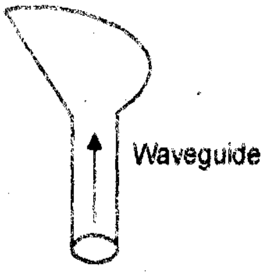
Microwaves are unidirectional; when an antenna transmits microwaves they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The microwave band is relatively wide almost 299GHz. Therefore wider sub-band can be assigned and a high data rate is possible.

On the other hand microwaves:

Propagation is line-of-sight. Since the towers with the mounted antennas needs to be in direct sight of each other, towers that are for apart need to be very tall. The curvature of the earth as well as other blocking obstacles does not allow two short towers to communicate using microwaves. Repeaters are often needed for long distance communication very high frequency microwaves cannot penetrate wall. Use of certain portion of band requires permission from authority. Parabolic dish antenna and horn antenna are used for this means of transmission.



(a) Dish Antenna



(b) Horro Antenna

Applications:

Microwaves are used for unicast communication such as cellular telephones, satellite networks and wireless LAN.

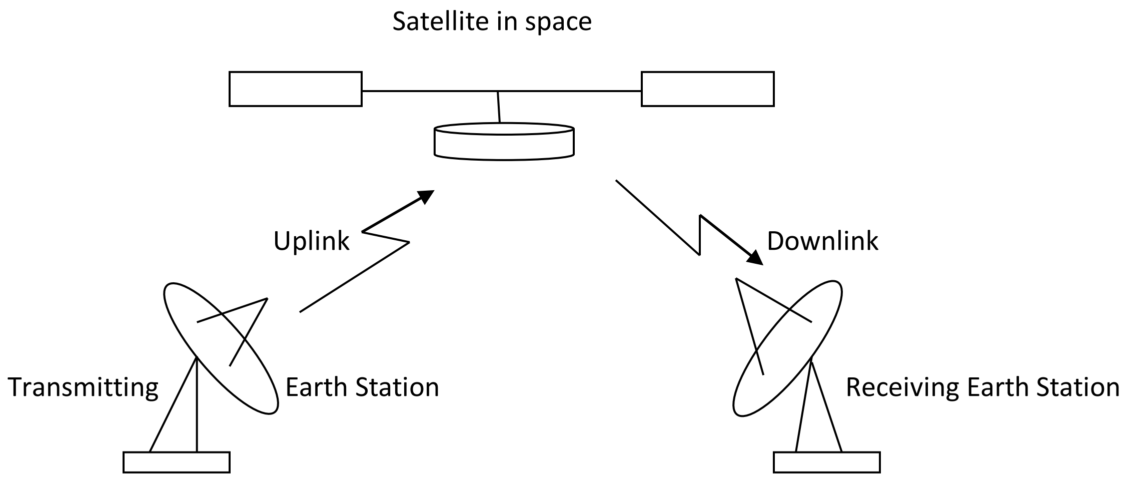
Infrared:

Infrared signals with frequencies ranges from 300 GHz to 400 THz can be used for short range communication. Infrared signals, having high frequencies, cannot penetrate walls. This helps to prevent interference between one system and another. In this, one room cannot be affected by the infrared waves in another room. However, the same characteristics make infrared signals useless for long range communications. In addition, we cannot use infrared waves outside a building because the sun’s rays contain infrared waves that can interfere with the communication.

Applications:

Infrared band, almost 400 THz, has an excellent potential for data transmission. So this will transfer digital data with a very high frequency. There are number of computer devices which are used to send the data through infrared medium e.g. keyboard mice, PCs and printers. There are some manufacturers provide a special part called the IrDA port that allows a wireless keyboard to communicate with a PC.

Communication Satellite:



Communication satellite acts as a relay station for communication signals. The satellite accepts data and signals transmitted from an earth station; amplify them and then retransmit them to another earth station. Earth stations use dish antennas to beam microwave signals to the satellites that amplify and retransmit the signals to other earth stations thousands of miles away. It use microwave radio as their telecommunications medium. Typically, high-earth orbit communications satellites are placed in stationary geosynchronous orbit approximately 22,000 miles above the equator. Satellites are powered by solar panels and can transmit microwave signals at a rate of several hundred million bits per second. Initially, communication satellites were used for voice and video transmission. They are now used for high speed transmission of large volumes of data. However they are not suitable for real-time processing because of the involvement of time delay caused by long distance. Many companies these days use networks of small satellite dish antennas known as VSAT (Very Small Aperture Terminal) to connect their stores and worksites via satellite.

Types of Computer Networks:

Local area network (LAN):

A LAN is usually privately owned network that links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home, office, or it can extend throughout a company and include voice, sound, and video peripherals. Currently, LAN size is limited to a few kilometers.

LANs are designed to allow resources such hardware e.g., a printer, software e.g., an application program, or data, to be shared between personal computers or workstations. In a LAN, we will find PCs, file server, DNS server, router, bridge, switch, hub, gateway, multilayer switches, printers, firewall and a lot of other connecting devices. Today LAN networks mostly used are Ethernet, Fast Ethernet (FE), Gigabit (GE) Ethernet, Token ring and FDDI. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Traditionally, LANs have data rates in the 4 to 16 Mbps range. Today, however speeds are increasing and can reach 100 Mbps with gigabit systems in development.

Metropolitan Area Network (MAN):

This is a larger network that connects computer users in a particular geographic area or region. The MAN network usually exists to provide connectivity to local ISPs, cable TV, or large corporations. It is far larger than a LAN and smaller than a WAN. Also large cities have metropolitan area networks. It is designed to extend over an entire city. It may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. For example, a company can use a MAN to connect the LANs in all of its offices throughout a city.

A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as a local telephone company. Many telephone companies provide a popular MAN service called Switched Multi-megabit Data Services (SMDS).

Wide Area Network (WAN):

A wide area network (WAN) provides long-distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, a continent, or even the whole world. The Internet is an example of a worldwide public WAN. Most WANs exist to connect LANs that are not in the same geographical area. This technology is high speed and very expensive to setup.

In contrast to LANs (which depend on their own hardware for transmission), WANs may utilize public, leased, or private communication devices, usually in combinations, and can therefore span an unlimited number of miles. A WAN that is wholly owned and used by a single company is often referred to as an enterprise network.

Bluetooth

Bluetooth is a specification for the use of low-power radio communications to wirelessly link phones, computers and other network devices over short distances. A Bluetooth is an ad hoc network, which means that the network is formed spontaneously. The name Bluetooth is borrowed from Harald Bluetooth, a king in Denmark more than 1,000 years ago. It was originally started as a project by the Ericsson Company.

Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets. Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters). Bluetooth devices generally communicate at less than 1 Mbps.

Bluetooth networks feature a dynamic topology called a **piconet** or **PAN**. Piconets contain a minimum of two and a maximum of eight Bluetooth peer devices. Devices communicate using protocols that are part of the Bluetooth Specification. Definitions for multiple versions of the Bluetooth specification exist including versions 1.1, 1.2 and 2.0.

Although the Bluetooth standard utilizes the same 2.4 GHz range as 802.11b and 802.11g, Bluetooth technology is not a suitable Wi-Fi replacement. Compared to Wi-Fi, Bluetooth networking is much slower, a bit more limited in range, and supports many fewer devices.

As is true for Wi-Fi and other wireless technologies today, concerns with Bluetooth technology include security and interoperability with other networking standards. Bluetooth was ratified as **IEEE 802.15** standard**.**

Wi-Fi

"Wi-Fi" is the nickname for Wireless Fidelity –a high speed internet and network connection without the use of wires, cables and other stuff. It is a popular technology that allows an electronic device to exchange data wirelessly using radio waves over a computer network, including high-speed Internet connections.

The Wi-Fi Alliance defines Wi-Fi as any wireless local area network (WLAN) products that are based on the IEEE 802.11(Institute of Electrical and Electronics Engineers) standards. However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".

A device that can use Wi-Fi such as a personal computer, video game console, Smartphone, tablet, or digital audio player can connect to a network resource such as the Internet via a wireless network access point. Such an access point is called hotspot which has a range of about 20 meters indoors and a greater range outdoors. Hotspot coverage can comprise an area as small as a single room with walls that block radio waves or as large as many square miles — this is achieved by using multiple overlapping access points.

Wi-Fi uses different security measures such as WEP, an earliest encryption protocol. But it is easily breakable. Therefore, much higher quality protocols, WPA and WPA2, were added later which provide robust security than the WEP.

Data Transmission

Data transmission, **digital transmission**, or **digital communications** is the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint communication channel. Examples of such channels are copper wires, optical fibers, wireless communication channels, and storage media. The data are represented as an electromagnetic signal, such as an electrical voltage, radio wave, microwave, or infrared signal.

Data transmission can be of two types:

i) Serial data communication
ii) Parallel data communication

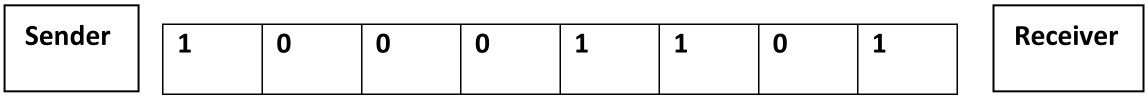
Serial communication:

A method of transmission in which data is sent one bit at a time is called serial transmission. The character bits are sent sequentially. Serial transmission is slower than parallel transmission as data is sent sequentially one bit at a time.

Digital serial transmissions are bits sent over a single wire. Because it requires less signal processing, less problem of data synchronization and less chance for error than parallel transmission, the transfer rate of each individual path may be faster. This can be used over longer distances as a check digit or parity bit can be sent along it easily.

The use of parallel communication for longer distance data communication is unfeasible for economic and practical reasons, eg: amount of extra cable required and synchronization difficulties, all long distance data communications takes place over serial connections.

Telephone lines use this method of data transmission. Each individual bit of information travels along its own communication path.



Parallel communication:

It is a method of sending several data signals simultaneously over several parallel channels. It contrasts with serial communication; this distinction is one way of characterizing a communications link. Thus in this transmission groups of bits are sent at the same time over multiple wires. It is usually unidirectional. Each bit is transmitted over a separate line.

Parallel transmission is faster because all bits are sent at the same time. For example: the internal transfer of data in a computer uses a parallel mode. The data transmission between computer and printer is done using parallel transmission.

Bit 0———————————————————————bit0

Bit1————————————————————————bit1

Bit2————————————————————————bit2

Bit3————————————————————————bit3

Bit4————————————————————————bit4

Bit5————————————————————————bit5

Bit6————————————————————————bit6

Bit7————————————————————————bit7

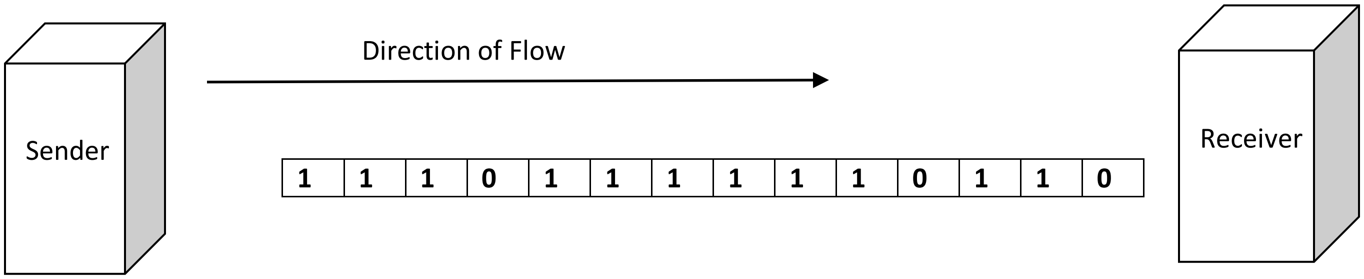
Sender ___________ Media _____________ Receiver

Synchronous Communication:

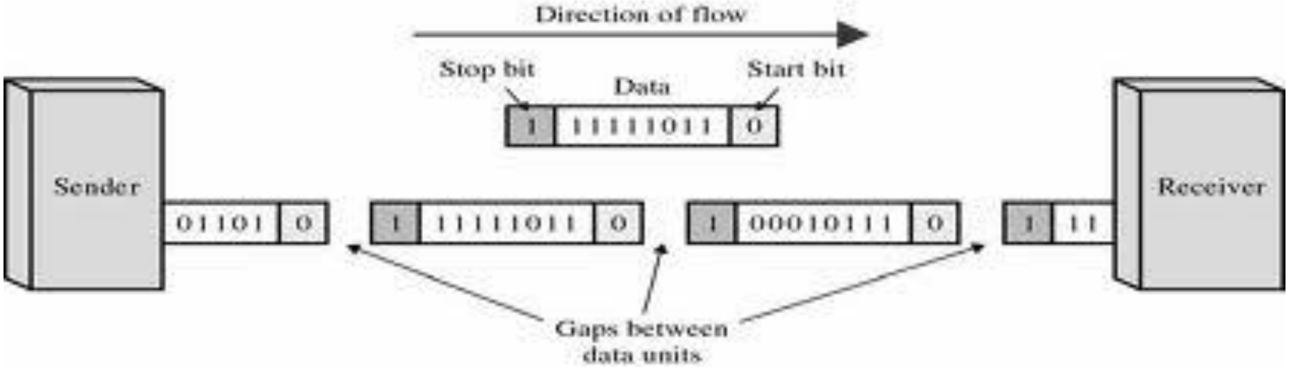
In Synchronous communication scheme, after a fixed number of data bytes a special bit pattern is send called SYNC by the sending end. It uses no start and stop bits, but instead synchronizes transmission speeds at both the receiving and sending end of the transmission using clock signal(s) built into each component.

Data transmission takes place without any gap between two adjacent characters. However data is send block by block. A block is a continuous stream of characters or data bit pattern coming at a fixed speed. We will find a Sync bit pattern between any two blocks of data and hence the data transmission is synchronized.

Synchronous communication is used generally when two computers are communicating to each other at a high speed or a buffered terminal is communicating to the computer. It is much faster than asynchronous because there is no gap between characters. This transmission is suited for remote communication between a computer and related devices like printers etc.



Asynchronous Transmission



In asynchronous transmission, data is transmitted character by character. It uses start and stop bits to signify the beginning of data bit. There are irregular gaps between characters in this transmission. It is cheaper to implement because data is not saved before it is sent.

It uses a special start signal. The signal is transmitted at the beginning of each message. The start signal is sent when the character is about to be transmitted.

A start bit has a value of 0. It is called space state. The value of 0 indicates that a character is about to be transferred. It alerts the receiver and it gets ready to receive the character. If start bit has a value 1, it indicates that the line is idle. It is also called mark state.

Network Topology

Network topology is the layout pattern of interconnections of the various elements such as links, nodes etc. of a computer network i.e. it refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate is determined by the network's topology.

Network topologies may be physical or logical. **Physical topology** refers to the physical design of a network including the devices, location and cable installation. **Logical topology** refers to how data is actually transferred in a network as opposed to its physical design. In general physical topology relates to a core network whereas logical topology relates to basic network (signal flow).

A LAN is one example of a network that exhibits both a physical topology and a logical topology.

Network topologies are categorized into the following basic types:

- Bus Topology
- Ring Topology

- Star Topology
- Tree Topology
- Mesh Topology

Bus Topology

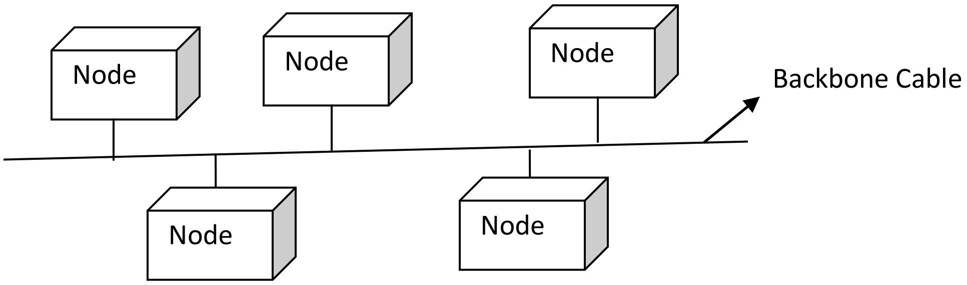


Fig: Bus Topology

Bus networks use a common backbone to connect all devices. A single cable, the backbone, functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

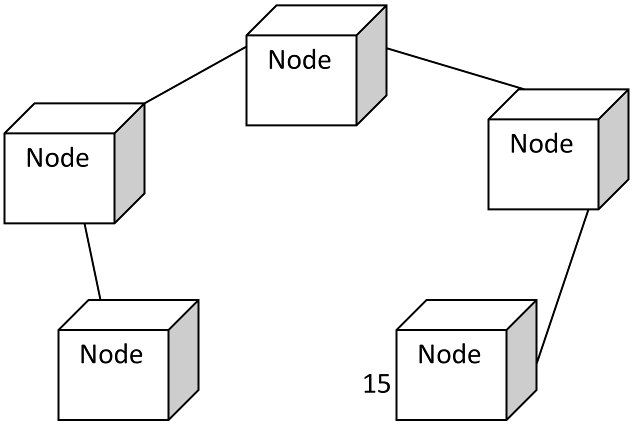
Advantages:

i. If any node or cable (except backbone) fails, it does not affect the whole network.
ii. They are relatively easy to install
iii. Don't require much cabling
iv. Easy to add and remove any node or cable except the backbone cable

Disadvantages:

i. If the backbone cable fails, the entire network goes down
ii. Since all the data are transmitted through the backbone cable, data traffic is high
iii. Bus networks work best with a limited number of devices

Ring Topology



In a ring network, every device has exactly two neighbors for communication purposes. All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise").

Advantages:

i. Short cables are required compared to other topologies

ii. It works where there is no central site computer system

iii. It is not dependent in a single cable or node

Disadvantages:

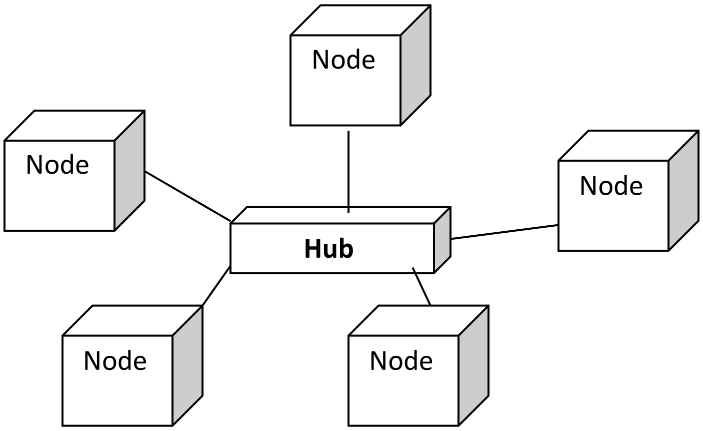
i. A failure in any cable or device breaks the loop and can take down the entire network.

ii. It is rarely used in modern LAN

iii. It is difficult to find out the error

iv. Adding and removing any node or cable is difficult

Star Topology



A star network features a central connection point called a "hub node" that may be a network hub, switch or router. All devices are connected to this central hub. Nodes communicate across the network by passing data through the hub. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet. Many home networks use the star topology these days.

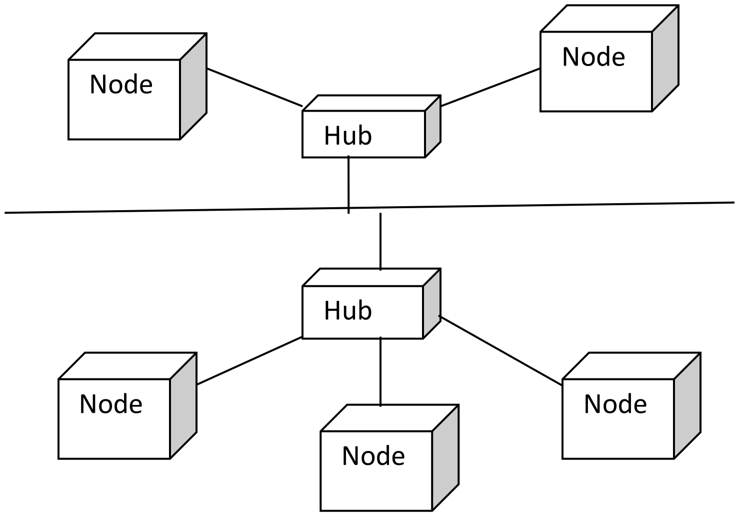
Advantages:

i. A failure in any node or cable will only take down one computer's network access and not the entire LAN.
ii. Easy to diagnose the fault
iii. Easy to add and remove a node or cable

Disadvantages:

i. Compared to the bus topology, a star network generally requires more cable
ii. If the hub fails, the entire network also fails

Tree Topology



Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the root of a tree of devices. In this topology, several computers are linked in a hierarchical fashion in the network. A node acting as a server in the higher level can act as a client in the lower level.

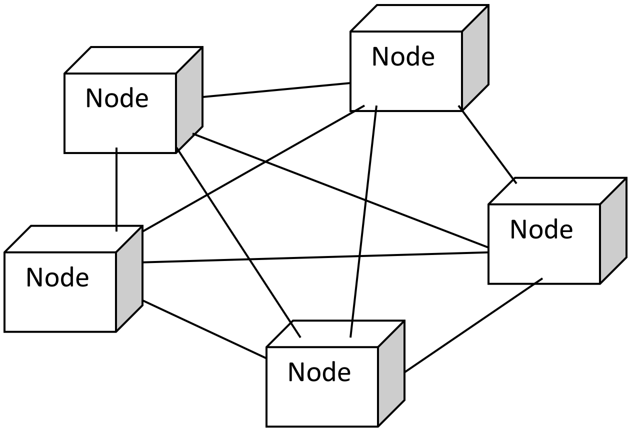
Advantages:

i. It supports future expandability of the network much better than a bus or a star.
ii. Failure in any single node does not affect the entire network.

Disadvantages:

i. If the main cable fails, entire network may go down
ii. Failure in the hub brings down all the nodes below it

Mesh Topology



Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. It has point-to-point connection between every node in the network. Some WANs, such as the Internet, employ mesh routing.

A mesh network in which every device connects to every other is called a **full mesh**. However, **partial mesh** networks also exist in which some devices connect only indirectly to others.

Advantages:

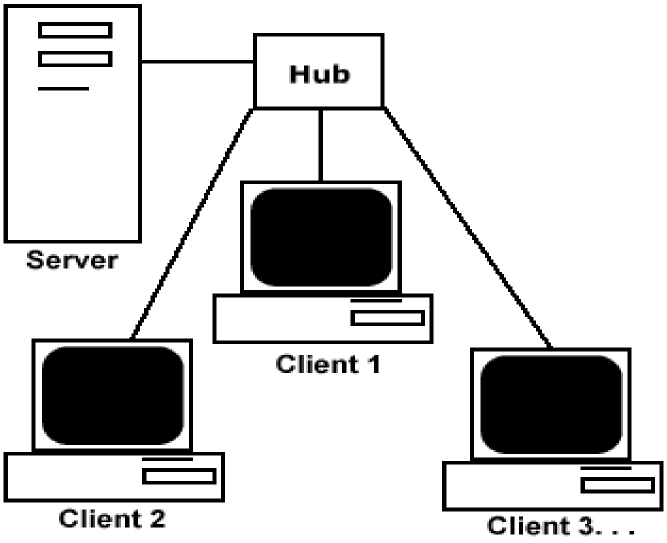
i. Failure in any one wire or node does fail the entire network
ii. It is the most secure topology
iii. Faster communication because of point-to-point connection

Disadvantages:

i. Most complicated network topology
ii. Expensive in comparison to other topologies.
iii. Difficult to find the error and trouble shoot.

Networks Architecture:

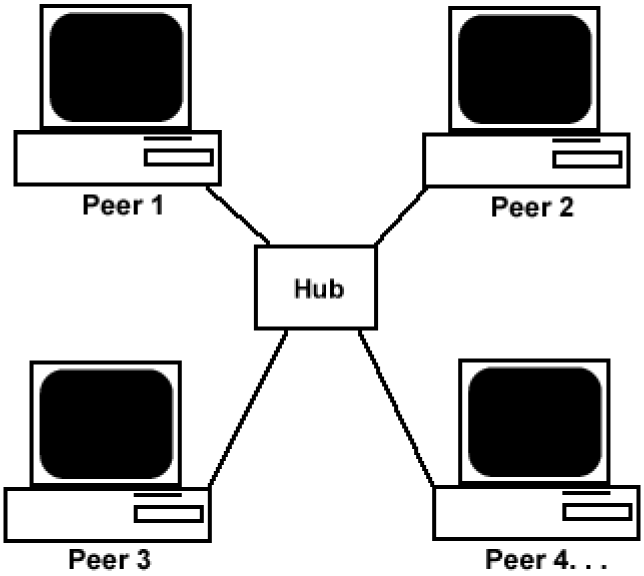
Client - Server Network Architecture:



It is network architecture in which each computer or process on the network is either a *client* or a *server*. It acts as distributed application which partitions tasks or workloads between the providers of a resource or service, called servers and service requesters, called clients. Servers are powerful computers with server OS or processes dedicated to managing disk drives (*file servers*), printers (*print servers*), or network traffic (*network servers)*. Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server machine is a host that is running one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests.

Peer -to- Peer Network Architecture (P2P):



P2P is a distributed application architecture that partitions tasks or workloads among peers. It is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler, but they usually do not offer the same performance under heavy loads. Here, each computer can act as a client or server for the other computers in the network, allowing shared access to files and peripherals without the need for a central server.

P2P networks can be set up in the home, a business or over the Internet. Each network type requires all computers in the network to use the same or a compatible program to connect to each other and access files and other resources found on the other computer. P2P networks can be used for sharing content such as audio, video, data or anything in digital format. The owner of each computer on a P2P network would set aside a portion of its resources - such as processing power, disk storage or network bandwidth -to be made directly available to other network participant, without the need for central coordination by servers or stable hosts.

Internet

The Internet is a system of linked networks that are worldwide in scope and facilitate data communication services such as remote login, file transfer, electronic mail, the World Wide Web and newsgroups. It is also called the network of network.

With the meteoric (dramatic) rise in demand for connectivity, the Internet has become a communications highway for millions of users. The Internet was initially restricted to military and academic institutions, but now it is a full-fledged medium for any and all forms of information and commerce. Internet websites now provide personal, educational, political and economic resources to every corner of the planet.

Intranet

With the advancements made in browser-based software for the Internet, many private organizations are implementing intranets. An intranet is a private network utilizing Internet-type tools, but available only within that organization. For large organizations, an intranet provides an easy access mode to corporate information for employees.

Extranet:

It can be defined as an extended intranet that links selected resources of a company with its customers, and other business partners, using the Internet or private networks to link the organizations' intranets. It is a secure network that provides controlled access to areas of each other's corporate intranets by remote authenticated parties.

VPN (Virtual Private Network)

VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access server on our workplace network. Using a VPN helps us save money by using the public Internet instead of making long–distance phone calls to connect securely with y private network. There are two ways to create a VPN connection, by dialing an Internet service provider (ISP), or connecting directly to Internet.

Protocols:

Network protocols are standards or set of rules that allow computers to communicate. A protocol defines how computers identify one another on a network, the form that the data should take in transit, and how this information is processed once it reaches its final destination. Protocols also define procedures for handling lost or damaged transmissions or packets. For example: TCP/IP (Transmission Control Protocol/internet Protocol). Although each network protocol is different, they all share the same physical cabling. It is actually the agreement between two or more communicating devices in the network.

Network firewall

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If we don't have a good idea of what kind of access we want to allow or to deny, a firewall really won't help us. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it. Administrators for firewalls managing the connectivity for a large number of hosts therefore have a heavy responsibility.

Connecting devices/Networking Devices:

These are the devices that connects two or more LANS, or segments with each other or with the Internet. These connecting devices can operate in different layers of the Internet model. Some of them are:

Hubs

It is a device that centrally connects devices in a computer network. There are two types of a hub i.e. active hub which is a multiport repeater that is used to create connections between stations in a physical star topology; and passive hub which is just a connector that connects the wires coming from different branches.

Every computer is directly connected with the hub. When data packets arrives at hub, it broadcast them to all the LAN cards in a network and the destined recipient picks them and all other computers discard the data packets. Hub has four, eight, sixteen and more ports and one port is known as uplink port, which is used to connect with the next hub. Hubs work at the physical layer of the OSI (Open System Interconnection) model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

Switches

Like the router, a switch is an intelligent device that maps the IP address with the MAC address of the LAN card. Unlike the hubs, a switch does not broadcast the data to all the computers; it sends the data packets only to the destined computer. Thus switches are more smart devices than the hubs. Switches are used in the LAN, MAN and WAN. In an Ethernet network, computers are directly connected with the switch via twisted pair cables. In a network, switches use the three methods to transmit the data i.e. store and forward, cut through and fragment free. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

Routers

A router is a communication device that is used to connect two logically and physically different networks, two LANs, two WANs and a LAN with WAN. The main function of the router is to sorting and the distribution (i.e. routing) of the data packets to their destinations based on their IP addresses. Routers provides the connectivity between the enterprise businesses, ISPs and in the internet infrastructure, router is a main device. Every router has routing software, which is known as IOS. Router operates at the network layer of the OSI model. Router does not broadcast the data packets. Routers connect two or more logical subnets, each having a different network address.

Gateway

A gateway can translate information between different network data formats or network architectures. They are also called **protocol converters** because a gateway can convert one protocol stack into another. For example, it can translate TCP/IP to AppleTalk. So computers supporting TCP/IP can communicate with Apple brand computers. Though they can operate at any layer of the OSI model, most gateways operate at the application layer, as well as operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. A routing machine is not a gateway, although it could be used interchangeably sometimes.

Repeater

A repeater connects two segments of the network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. It can extend the physical length of a LAN.

Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

Bridge

A bridge works in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) address contained in the frame. A bridge has a filtering capabilities i.e. it can check the destination address of a frame and decide if the frame should be forwarded or dropped.

A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures.

Bridge Router or Brouter

A **Bridge Router** or **brouter** is a network device that works as a bridge and as a router. The brouter routes packets for known protocols and simply forwards all other packets as a bridge would.

Brouters operate at both the network layer for routable protocols and at the data link layer for non-routable protocols. As networks continue to become more complex, a mix of routable and non-routable protocols has led to the need for the combined features of bridges and routers. Brouters handle both routable and non-routable features by acting as routers for routable protocols and bridges for non-routable protocols. Bridged protocols might propagate throughout the network, but techniques such as filtering and learning might be used to reduce potential congestion. Brouters are used as connecting devices in the networking system, so it acts as a Bridge in a network & as a Router in an Internetwork.